THE ISSUES IN THE COLLECTION, VERIFICATION AND ACTIONABILITY OF CITIZEN-DERIVED AND CROWDSOURCED INTELLIGENCE DURING THE RUSSIAN INVASION OF UKRAINE, 2022

UDC 355.404.5:(470)(477)“2022”
https://doi.org/10.53679/2616-9460.specialissue.2022.09

Paul Burke
Director of Global Projects
for Glengulf International, United Kingdom
ORCID: 0000-0002-8764-7266

When Russia invaded Ukraine on 24 February 2022, a war was opened on four fronts simultaneously, in the North, the East, the Southwest and the South. With Ukrainian troops immediately committed to battle along multiple axes of Russian advances, the importance of accurate and actionable Intelligence was key from the start. Alongside the usual military and civilian elements of the Ukrainian Intelligence community were Ukrainian citizens desperate to contribute what they were seeing and hearing on the ground as the invasion unfolded. Tools were rapidly made available for citizens to report sightings of Russian military activity, which were then verified and processed by Ukrainian Intelligence and where possible, were turned into actionable end-product reporting for military targeting. Such citizen-derived or crowdsourced Intelligence has provided an additional strand of source reporting for Ukraine during the conflict, yet its collection and use is not without its issues. Ethical issues are created, such as citizens putting themselves in ever-greater danger to collect information which they believe may be useful. This creates an additional problem of the potential attribution by the aggressor, of such a citizen as an informant, along with the concomitant risks which that brings. Policy needs to sufficiently incorporate citizen Intelligence to allow actions to be taken based on this product, especially lethal strikes. Practical issues include an increased volume of raw material for human analysts to process, before actionable Intelligence can be produced. This paper addresses these issues and signposts additional issues that require further research.

Keywords: Intelligence, crowdsourcing, CITINT, Ukraine invasion, Space, ground collection, attribution, IMINT.

---

1 Dr. Paul Burke is an Intelligence and counter-terrorism professional with 30 years of strategic experience in managing the Intelligence and security domain primarily within UK government. Holding a Doctorate in Policing, Security & Community Safety, and an MA in Intelligence Studies, he previously worked as UK National Intelligence Adviser on Counter-Terrorism, based in British Embassy Baghdad, working within Iraq’s Ministry of Interior (2004–2006), and as UK National Intelligence Mentor on Counter-Narcotics in British Embassy Kabul (2007–2009). After a career in the UK Armed Forces and government service, he joined technology company IBM where he was the Dubai-based Head of National Security and Public Safety for the Middle East and Africa region. Following this, he became Director of Global Projects for Glengulf International where he focused on managing a programme of counter-terrorism capacity building in Mogadishu, for the Somali Police, Intelligence agencies and the Armed Forces. He was the Senior Researcher in a European Research Council Advanced Grant project on counter-terrorism in liberal democracies. This 5-year project was directed by Professor Seumas Miller, a global leader in the field of applied ethics. Along with Prof. Miller and Dr. Elnakhal, he is the Editor of “Global Jihadist Terrorism – Terrorist Groups, Zones of Armed Conflict and National Counter-Terrorism Strategies” (Burke et al., 2021).
THE ISSUES IN THE COLLECTION, VERIFICATION AND ACTIONABILITY OF CITIZEN-DERIVED AND CROWDSOURCED INTELLIGENCE DURING...
ple would be a Ukrainian farmer in a remote region who drives past a group of Russian armoured vehicles, then photographs or records a video of it, and either uploads the photo to his social media feeds or sends it directly to the Ukrainian government’s portal designed to collate information on Russian military activities within Ukraine. The rapid progression of technology, especially of social media platforms, mobile messaging applications and the capabilities of handheld devices such as mobile phones and unmanned aerial systems (UAS), has created an extremely powerful reporting ability for the average citizen, especially in the developed world where the latest model of iPhone sells for considerably more than a laptop computer. The joint capabilities of citizens to provide real-time reporting on unfolding events, coupled with their ability to capture these events in very high-resolution photographs or 4K (and now 8K) video format that are embedded with evidentially crucial data such as time stamps and geo-reference data, means that a richly detailed and potentially verifiable source of Intelligence has now become available to State-level Intelligence agencies.

“Ground Collection” by citizens

The exponential increase in the popularity of social media platforms in the last 15 years has resulted in the oft-heard comment that “we are all journalists now” (Gant, 2007; Rosenblum, 2017; Servaes, 2009). While this is not entirely accurate, a similar claim might be made that “we are all Intelligence collectors”. The inherent problems with both statements are remarkably similar, covering issues including, but not limited to, verification of information, vulnerability to innocently reporting and thus propagating deliberate disinformation, provenance of reporting, being appropriately trained to conduct such work, quality of the raw information reported, and individuals taking unacceptably high risks to collect information which may be low-grade or even worthless. A more accurate comparison may lie within a US Army philosophy following the 2003 invasion of Iraq, which decreed “every soldier a sensor” (Department of the Army Headquarters, 2007). Before the Russian invasion began on 24 February 2022, the Ukrainian Ministry of Digital Development already had an IT application for civil society, named “Diiia”, which was designed to be “a central hub for citizens’ interactions with their government, allowing someone to access their identity cards, pay their taxes, and receive public services” (Druziuk, 2022). This app was repurposed to allow Ukrainian citizens to provide real-time reporting of Russian military troop dispositions, movements, strengths and equipment.

Initially successful, it was soon targeted by Russian spambots that began to flood the Diiia system and to make it difficult for genuine tip-offs to be filtered from the flood of spam. Ukraine’s response was to rapidly re-tool the app, adding a chatbot called e-Voroh (or e-Enemy), requiring a Ukrainian citizen to log in using his national identity credentials, before posting a tip-off. This counter-measure was further strengthened through the use of an associated channel on the Telegram messaging application, to allow further information to be solicited, thus providing a fine filter, on top of the coarse filter of requiring a validated log-in (Bussoletti, 2022). The Ukrainian government actively encourages its citizens to report sightings and information on Russian military activity through the use of the app and by the end of the fifth week of the Russian invasion, more than 200,000 sighting reports had been made using e-Voroh (Aroged, 2022). While the provision of such “citizen Intelligence” (for the sake of simplicity we shall refer to this as CITINT) has undoubtedly made a positive impact in the first few months of the Russian invasion, it nevertheless raises important questions about the collection and use of this source.

The attribution of citizen actions and the associated issues of legality

It is likely that the issue of attribution of CITINT may need addressing within a conflict, on a continuous basis. If an individual or a group conducts their own ground collection of information, and this is either web-scraped by NATO and subsequently used to conduct a strike on a target derived from this collected Intelligence, to what degree, if at all, is the source attributable to NATO? On a sliding scale, this could increase in complexity and potential attribution. For example, if a source such as our farmer was cognitive of that fact that, every time he published detailed photos of deployed enemy armoured assets, an artillery or drone strike targets this armour soon afterwards, he may be spurred on to travel further and actively seek out more targets to photograph and publish. This activity could potentially result in the attribution of the farmer becoming increasingly closer. Various anecdotes provide examples of citizen-derived sabotage of Russian assets, following the invasion of Ukraine. In February 2022, a Ukrainian crew member partially sank a Russian oligarch’s super yacht in protest at the invasion (Burgen, 2022) while in Belarus, rail workers, cyber-hackers and other activists have carried out acts of sabotage to prevent rolling stock from transporting Russian armoured vehicles and troops to the Ukrainian border (Augusteijn, 2022; Ball, 2022; Vasilyeva, 2022).
What are the challenges in attributing and verifying citizen-provided Intelligence?

Every Intelligence source is necessarily subject to a verification process (subject to the usual operational constraints, which may negate this to almost zero in some circumstances). Open Source Intelligence (OSINT) in general, and CITINT in particular, are no different in this respect. The so-called “Five Vs of big data” affect CITINT just as they do for sensitive source collection. The volume of data can be so great that it overwhelms analysts attempting to find meaningful items in a vast pile of raw information. The example provided above, with the initial Ukrainian CITINT portal being inundated by Russian spambots, illustrates this aptly. Next, the veracity of the information can be difficult to confirm and is almost always a time-consuming affair when human analysts are involved (although this is one area in which progress is being made, with ongoing improvements being achieved in the speed and accuracy of artificial intelligence systems’ capabilities in sifting big data). CITINT has the potential to be verified through crowd-sourcing, with large numbers of citizens able to look at an image or video clip and confirm or deny the location of the subject (Bergengruen, 2022; Herbekovitz, 2020; Kostenko, 2022; Stottlemyre, 2015). The variety of data can create an issue in collection where the raw product may be structured, unstructured or semi-structured, but in the case of the Ukrainian Diia app, this issue appears to be more minor, given that subscribers posted photos, video footage and text comments of their sightings. This was further mitigated by the introduction of the additional national ID login policy described previously.

The velocity at which the information arrives can equally overwhelm the filtering and analysis process. During a period of very intense activity, it is possible for an Intelligence system to be overloaded to the point that it new reports cannot be generated, due to the speed at which updates are coming into the various systems. Finally, the value of information is closely related to the “so what?” question, as there is little cost-benefit advantage in collecting, verifying and analysing raw information if 99 % of it has no value to the Intelligence consumer. The value of this information can be adversely affected by any of these other “V factors” and this can have a greater negative impact at the tactical end of the scale. The importance of Intelligence reporting on enemy troop dispositions, for example, can rapidly degrade over a short period of time, especially in a highly dynamic battlespace.

1 This is also seen as the “Four Vs”, depending on the Author.

CITINT and the use of Space

As one of the five domains of warfare, Space has become a key battlespace for armed forces in modern conflict, and it has equal importance for CITINT. Operation DESERT STORM in 1991 has widely been described as “the first space war”. Walker et al. (2003) state that this was because “every aspect of military operations depended, to some extent, on support from space-based systems... the assistance rendered was invaluable and the new technology, combined with Air-Land Battle Doctrine, changed the way the Army fought. The conflict represented a watershed in the development of these systems” (Walker et al., 2003, p. 150). Corporate providers now provide not only high-resolution imagery, but also the analysis of it and the end-product, if required, often filling gaps which State-level agencies cannot fill quickly. Ten commercial satellite operations companies make up a consortium that works closely with US Space Command on topics such as threats to satellites and fallback communications systems.

The race for Space no longer involves only superpowers vying for superiority, the new giants of the Space race are private sector companies such as Maxar, SpaceX and Virgin Galactic. The agility of the corporate sector to invent, innovate, adapt and take risks far surpasses that of the military-industrial sector and it is in this corporate realm that much of the innovation will be accomplished.

SpaceX, Elon Musk’s company, has launched more than 100 satellites into space from one launch vehicle, increasing the number of satellites far more quickly than most governments could hope to achieve (Mack, 2021) “abstract”: SpaceX lifted a record-breaking number of satellites in a single payload when its Transporter-1 ride-share mission blasted off from Cape Canaveral in Florida at 7 a.m. PT (10 a.m. ET. Musk’s Starlink system now constitutes the biggest commercial satellite constellation in the world, with over 2,500 low Earth orbit satellites deployed at the time of writing, and with ambitions plans to launch a further 42,000 satellites. To put that into perspective, it is 15 times the number of all satellites currently in Space (Yan Huang et al., 2021). The provisioning of the Armed Forces of the Ukraine with Starlink-enabled communications platforms has been a game-changer for Ukrainian troops on the ground, and a lifeline for communities whose...
infrastructure has been shattered by the conflict (Walt, 2022). Mega-constellations like Starlink can function as a force multiplier, as its use in Ukraine has ably demonstrated, and it has proven highly resistant to the efforts of Russian Electronic Warfare (EW) units to jam the terminals or the signal (U.S. Senate Committee on Armed Services, 2022; Defense Express, 2022; Miller, C. et al., 2022). The Starlink system provided essential communications for the defenders of the Azovstal complex in Mariupol, home to the last enclave of Ukrainian resistance in the heavily-besieged city before it fell to Russian troops in May 2022. Once Starlink was enabled, the defenders could continue communicating uninterruptedly with their chain of command and with loved ones, even within the depths of the factory’s bunker system.

In a similar way to OSINT and CITINT, the Ukrainian conflict is signposting that Space-based Intelligence and warfare is also coming of age. While capabilities such as the first Talent Keyhole (TK) satellites opened the door to high-resolution imagery of then-Soviet capabilities, the contemporary push into space by the private sector has supercharged the capabilities of real-time Intelligence provision. The ability of citizens to derive actionable Intelligence from this source will continue to increase as its technological capabilities expand.

How will Imagery Intelligence (IMINT) be affected?

The training of a typical IMINT analyst is a lengthy process which has traditionally focused on the end-product of SECRET and ‘TOP SECRET’ source material. Platforms such as the U2, RIVET JOINT (RJ) and satellites provide extremely high-resolution imagery with extremely precise geolocational information, often in 3D stereoscopic format. Assessing the provision of photos and video uploaded to social media platforms creates an additional work strand for IMINT analysts. Despite the ability to record in 4K or 8K video from modern smartphones, much footage will be of sub-optimal quality compared to traditional IMINT product, and this may require digital cleaning and editing before it can be fully analysed and verified. While a citizen-uploaded photograph lies at one end of the spectrum, at the other end are the commercial companies providing very high-resolution imagery, especially those producing imagery from synthetic aperture radar (SAR) satellites or in niche areas such as the radio frequency (RF) detection of electronic jammers being used to deny or degrade the ability to use GPS or communications systems (Datta, 2022).

Although systems such as these may cloud the distinction of whether they constitute OSINT or not, what is very clear is the increasing use of citizens, either as individuals, collective groups or companies such as Bellringcat, to take the commercial end-product from corporate suppliers of imagery and other information, and to conduct their own analysis on it. This has produced CITINT reports on the imminence of the Russian invasion of Ukraine in 2022, incontrovertible evidence that the murders of civilians in the town of Bucha were carried out while Russian troops were based there (and not after their departure, as claimed by Russian media), and detailed evidence of mass graves being dug and then afterwards filled in to hide evidence of potential war crimes (Roth & Ruesch, 2022). A senior NGA official succinctly provided a signpost to the increasing use of CITINT in the near future, saying that “…since everyone can obtain commercial imagery and data, the advantage will come from turning data into analytic insights” (Werner, 2021). The increase in CITINT, and also commercial imagery, as a source of Intelligence will require changes in the training and mentoring of IMINT analysts, if the potential benefits of CITINT imagery are to be fully exploited. Indeed, the National Geospatial-Intelligence Agency confirmed as much, noting that the introduction of new sources and capabilities into the IMINT arsenal will require “a strategic shift in mindset… It also will take time for intelligence analysts to become accustomed to turning to commercial sources first…because commercial data is unclassified, reports produced with those data are easier to share and individual datasets may be easier to fuse with other datasets” (Defense Express, 2022).

That said, the advances in machine processing of imagery are constantly improving and the benefits that more refined artificial intelligence (AI) can bring will only increase with time. The speed at which information can be turned around into actionable Intelligence is highly dependent on whether the collection, analysis and dissemination systems lie closer to the agile end of the scale or to the more ponderous end. Even accredited HUMINT assets can be ponderous, in terms of being tasked and debriefed. A U2 or Rivet Joint (RJ) or similar airborne platform can collect extremely high-quality product but the lag between collection and actionable use can be considerable. A series of accurately geo-referenced photographs or videos, uploaded by a citizen, showing tanks and armoured vehicles in a laager location can potentially be processed and made actionable within minutes, subject to some of the constraints outlined above.

If sent directly to a dedicated hub such as Ukraine’s Dlia app, the information could be confirmed as non-
spam through the citizen log-in, verified by a drone from the nearest friendly unit and coordinates provided to artillery or other Joint Fire elements to conduct a fire-strike on the confirmed coordinates within minutes. Even if the information is not posted directly to a dedicated hub but is instead posted on social media, the information can still be scraped by web tools, and the targeting process continues as normal. With the US-supplied, current-generation Switchblade 300 and 600 drones, the same drone can be used to conduct the confirmation of the coordinates and then to carry out the strike, hence this platform is often referred to as a “kamikaze drone”. The same CITINT can also be used in a post-strike capacity to provide battle damage assessment (BDA), to allow friendly forces to confirm the effectiveness of the strike, whether the target vehicles are rendered inoperable, provide casualty figures, etc. The more accurately the BDA can be reported, the clearer the picture will be for assessing what losses the Russian forces have suffered. This further aids in the extrapolation of estimating combat losses from the assessed number of opposing troops committed to battle.

Is this a pivotal moment in the coming of age of OSINT as a discipline?

The Russian invasion of Ukraine is arguably the first major conflict in which OSINT has played such a significant part from the very start of the conflict. Traditionally looked down on as the “poor relation” of other Intelligence disciplines, OSINT has had to fight hard to make itself heard within the corridors of power, both within the Agencies themselves and to a certain extent by senior policymakers cleared to receive Secret and Top Secret Intelligence. The relationship between the speed of collection, the time-to-process, the importance and the relevance of the collected information has been dynamically altered since the start of the 2022 invasion. Before Russian vehicles had even crossed the Ukrainian border, and before any announcement on the Russian invasion was made public, academics and their students were analysing Google Maps traffic views on the main arterial roads into Ukraine (Lerman, 2022). A series of real-time Tweets documented what they assessed as a large column of Russian armour and vehicles beginning to move along a road leading from Belgorod, Russia, and crossing their Start Line into Ukrainian territory (Lewis, 2022).

The drive to embrace OSINT (and CITINT) more widely and more enthusiastically is likely to expand significantly in the new reality of the post-invasion environment, with a cost-benefit dividend leaning far more clearly towards the black than the red side of the investment ledger. In the perpetual search for more Intelligence bang for publicly-funded bucks, OSINT in general, and CITINT in particular, seem to offer an attractive rate of return. A drive to invest in, and embrace, OSINT and CITINT would produce significant benefits for NATO and EU nations, allowing them to exploit languages, skills and topography knowledge which would, in turn, improve the processing, exploitation and dissemination (PED) of actionable Intelligence. This in turn would result in considerable restructuring, especially for NATO Intelligence structures, their staffing and training requirements, and PED responsibilities. It would also potentially allow NATO to open up an opportunity for NATO to amalgamate the PED process, post-collection.

As the conflict in Ukraine unfolds and both sides dig in for what may develop into a more static war of attrition, the practical application of CITINT on the battlefield will be further shaped and refined. It is important that NATO and the EU are sufficiently agile willing to extract and learn from the bloody and costly battlefield experience of the Armed Forces of Ukraine, who are providing the real-time lessons of citizen-derived battlefield Intelligence. If OSINT (and CITINT) has truly come of age in the Ukrainian conflict of 2022, it will have important implications for the recruitment, selection, training and career path for Intelligence analysts within the Armed Forces of NATO and EU member states.

What are the risks and ethical issues involved in CITINT?

On 08 March 2022, the Security Service of Ukraine tweeted a report that they had used information provided through the dedicated Telegram channel for tip-offs, to conduct a successful strike against Russian military vehicles located outside Kyiv. The tweet carried a photograph of the immediate aftermath of the strike, showing destroyed Russian military vehicles on fire (Security Service of Ukraine, 2022). If CITINT is used to cue the targeting process for lethal strikes by Joint Fires, then it follows that the legal, practical, policy and ethical implications should be sufficiently considered to incorporate this into formal policy, particularly for NATO and EU member states. Individual member states should also, ideally, be satisfied that their national policies are sufficiently robust and watertight to allow for the use of such cueing, without the worry of the associated legal, ethical and practical considerations. If we consider our farmer, there are various risks in his collection and reporting of CITINT. Inspired by the early success of his first reports, which resulted in effective targeting of enemy armour, he may...
travel further afield and move from “bystander collection” to “hunter collection”, where he actively seeks out enemy locations in order to report their locations, strengths and equipment types through the web-based portal. He may begin to consider himself a covert asset, moving from a casual reporter of observed activity to a self-tasking role more closely associated with the work of a Covert Human Intelligence Source (CHIS) (in UK terms, at least). This could greatly increase the level of his personal risk, as he would be undertaking Intelligence collection work without any formal training, without the protection of being a member of the Armed Forces and potentially laying himself open to espionage charges. The recent death sentences handed out by unlawful “kangaroo courts” to foreign-national soldiers legally serving in the Armed Forces of Ukraine show the very real risks that a citizen may face, especially those operating in areas under the occupied control of Russian forces.

Currently, there does not appear to exist a general framework for the ethical issues in the use of CITINT to conduct lethal strikes on the battlefield. Probably the largest and most useful contributions in this field come from the work of Miller and Regan, who individually and together have written in detail on areas such as the ethical dimensions of the response of liberal democracies in combating terrorism, the ethics of National Security and Intelligence, and the ethics of the use of lethal force by Law Enforcement agencies (Miller, S. 2006, 2008, 2014, 2016; Miller S. et al., 2022; Miller, S. & Makela, 2005; Regan, 2008, 2013). Further research is currently ongoing in this area, with the aim of providing an in-depth examination of the issues around CITINT and from this, the derivation of a recommended framework of ethical and practical guidelines for use by NATO and EU member states (Burke et al., 2022).

How does CITINT fit into sub-threshold warfare?

The grey area of sub-threshold warfare is able to comfortably accommodate CITINT. Difficult to define by its very nature of murky greyness, this is the pseudo-battlespace in which adversaries are not directly engaged with each other’s troops but one or both parties are participating in the conflict in other ways, while stopping short of engaging in direct warfare. NATO and EU countries, together with others such as Australia, Canada and New Zealand, have provided assistance to Ukraine across a wide realm of sub-threshold support including financial donations, the supply of weapons platforms and ammunition, training, Intelligence support and communications architecture. The amount of this collective package is truly massive, with the US alone approving a package of aid worth $US 40 billion in May 2020 (Blinken, 2022). Without actually engaging in battle with Russian forces, and thus by definition stopping short of actual war fighting, Western nations have enabled Ukraine to inflict devastating losses on the occupying Russian troops. On 15 May 2022, the UK Ministry of Defence daily Defence Intelligence assessment on Ukraine assessed that, Russia had “likely suffered losses of one-third of the ground combat force it committed in February” (UK Ministry of Defence, 2022). The combination of the ability of Ukrainian citizens to provide accurate “ground collect” in contested areas, with the State-level agencies and their allies already providing tactical, operational and strategic Intelligence, is a powerful enabler of the weapons and supplies flowing into Ukraine from supportive countries. The military aid and the Intelligence-led use of it on the battlefield act as a mutually reinforcing, virtuous circle.

In recent conflicts, the nature of such sub-threshold warfare has changed, with operational support creeping ever closer to the red line of direct warfare. Russia has relied heavily on assets such as the Wagner Group during its military support operations in Syria and elsewhere. One advantage of using proxies such as the Wagner Group lies in their official deniability and the group is believed to have been active in training and instructional missions in other location such as the Central African Republic, Burkina Faso and elsewhere. Such sub-threshold warfare has led to rapid innovations in battlefield weaponry, with the UK, for example, believed to have modified the BRIMSTONE anti-armour weapon “within a matter of days” to allow it to be launched from a tractor. Subsequent video feeds showing the simultaneous destruction of two Russian tanks within days of this modification being introduced (Kadam, 2022).

Conclusion

This paper has taken a broad overview of the topic of citizen-derived Intelligence and attempted to highlight some of the nascent issues faced when collecting and using this source. Dedicated web-based portals
and apps can make the reporting of CITINT quicker and easier, while verification overlays such as national identity logins can drastically reduce the ability of adversaries to either flood the portal with spam or to hack it and electronically take it down. The effectiveness of CITINT has been proven through its use in Ukraine, with the successful targeting of Russian military targets based on photographic and video content embedded with accurate coordinates that can be verified through ancillary means such as military or even civilian drones. Space-based platforms are providing imagery at levels previously reserved for sensitive Intelligence. In 2006, imagery at 2-metre resolution was provided by the US to allies in the post-war insurgency in Iraq, whereas now corporate providers can provide 15 cm resolution as a paid product (Formeller, 2020) helping them identify smaller features on the ground to make more informed decisions from satellite imagery. 15 cm HD is created by applying our proprietary HD technology to our native 30 cm imagery. HD technology intelligently increases the number of pixels through a complex mathematical model that is tuned to the specific requirements of our imagery, resulting in a superior visual experience. This innovation will produce well-defined features and help both people and algorithms better extract meaningful information. Today, 15 cm HD is available for our satellite imagery products (View-Ready and Map-Ready products. There will be a necessary training overhead to enable the IMINT community to absorb the civilian-provided technologies but the benefits to this are clear.

Attribution of CITINT will always be a requirement but arguably no more than other sources and methods. A grey area is the potential attribution of a provider of Citizen Intelligence and much may depend on the way in which an adversary treats its opponents. The recent death penalties handed down by the illegal courts of the self-styled Donetsk to foreign members of the Ukrainian Marines, who are legally entitled to be treated as Prisoners of War (POWs) under the Geneva Convention, illustrates the risks to a potential collector of CITINT in Ukraine. If a uniformed member of a recognized Armed Forces can be sentenced to death in breach of international conventions such as the Geneva Convention, the risks to a civilian are far greater. If any further indication is needed, we need only look at the massacres carried out in Bucha. There are clearly a number of ethical issues involved in CITINT, in particular the collective moral responsibility issues and further research should help to clarify some of these problems, while also contributing to a framework of guidelines for CITINT conduct.

Other questions remain, which are outside the scope of this paper, including areas such as the use of AI and machine learning to filter information in the Intelligence chain, and to what extent the algorithms are visible and understandable. Last but not least is an analysis of the clearly major policy implications regarding automation, ethics, legality and boundaries of operation, especially considering capabilities such as automated drones and CITINT portals. The previously-mentioned concept of “every soldier a sensor” made perfect sense in the 1991 battlespace of the war in Iraq. I contend that this concept could be re-tooled for the post-Ukraine invasion period as “every citizen a collector” (Burke et al., 2022).

References

BBC. (2022, July 04). How many Ukrainians have fled their homes and where have they gone? BBC News. https://www. bbc.co.uk/news/world-60555472


Halpert, M. (2022, May 04). Russia’s invasion has cost Ukraine up to $600 billion, study suggests. Forbes. https://www.forbes.com/sites/madelinelhalpert/2022/05/04/russia-invasion-has-cost-ukraine-up-to-600-billion-study-suggests/?sh=3df1515b2dda


Lewis, J. (@Dr. Jeffrey Lewis). (2022, February 25). According @googlemaps, there is a ‘traffic jam’ at 3:15 in the morning on the road from Belgorod, Russia to the Ukrainian border. It starts *exactly* where we saw a Russian formation of armor and IFV/APCs show up yesterday. Someone’s on the move [Tweet]. Twitter. https://twitter.com/armscontrolwonk/status/149665781674036616


